Doc Code: AP.PRE.REQ

PTO/SB/33 (07-05)
Approved for use through xx/xx/200x. OMB 0651-00xx
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional)
5577-220 (IBM 018 PA)

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)] or facsimile submtted to 571-273-8300.
on _____

Signature_____

Typed or printed name _____

Application Number	Filed
09/764,252	01/17/2001

First Named Inventor
James Russell Godwin et al.

Art Unit	Examiner
2154	Ashokkumar B. Patel

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

☐ applicant/inventor.

☐ assignee of record of the entire interest.
See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed.
(Form PTO/SB/96)

☐ attorney or agent of record.
Registration number _____.

☑ attorney or agent acting under 37 CFR 1.34.
Registration number if acting under 37 CFR 1.34 46,867

/Thomas E. Lees/
Signature

Thomas E. Lees
Typed or printed name

937/438-6848
Telephone number

January 29, 2007
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required.
Submit multiple forms if more than one signature is required, see below*.

☐ *Total of _____ forms are submitted.

This collection of information is required by 35 U.S.C. 132. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11, 1.14 and 41.6. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	: Godwin et al.
Serial No.	: 09/764,252
Filed	: January 17, 2001
Title	: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR PROVIDING DATA FROM NETWORK SECURE COMMUNICATIONS IN A CLUSTER COMPUTING ENVIRONMENT
Attorney Docket	: 5577-220 (IBM018PA)
Examiner	: A. Patel
Art Unit	: 2154
Confirmation	: 8043

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

ARGUMENTS IN SUPPORT OF PRE-APPEAL BRIEF REQUEST FOR REVIEW

This paper is submitted with the applicants' Notice of Appeal and Pre-Appeal Brief Request for Review in response to the Office action made Final dated October 27, 2006.

Status of the Application

Claims 1, 3-9, 20, 22-28, 39, 41-47, 58-72 stand rejected under 35 U.S.C. § 112, second paragraph. Claims 1, 7, 20, 26, 39, 45 and 58-72 stand rejected under 35 U.S.C. §102(e) as being unpatentable over U.S. Pat. No. 6,266,335 to *Bhaskaran*. Claims 3-6, 8, 9, 22-25, 27, 28, 41-44, 46 and 47 stand rejected under 35 U.S.C. §103(a) as being unpatentable over *Bhaskaran* in view of U.S. Pat. No. 6,826,559 to Shaffer et al. (hereinafter, *Schaffer*).

Arguments

The applicants would like to extend thanks to Examiner Patel for courteously reviewing applicants' Reply to the Final Office action, mailed January 02, 2007 to provide a status before the end of the shortened statutory three month period for reply. The Examiner indicated that an Advisory Action will be mailed, which is confirmed in Public PAIR as of January 27, 2007. However, the action has not been mailed.

35 U.S.C. §112, second paragraph

During a telephone conversation between Examiner Patel and Thomas Lees, on behalf of the applicants, on January 26, 2007 in response to the applicants' status inquiry, Examiner Patel indicated that the rejection under 35 U.S.C. §112, second paragraph was suitably addressed in the reply of January 02,

2007 to the final Office action. To briefly review that rejection, the Examiner argued that there is insufficient antecedent basis for the recitation of "network communications" in each of independent claims 1, 20 and 39 because it is unclear how other "types" of communications recited in the claims are associated with network communications. The Examiner further argues that there is insufficient antecedent basis for the recitation of "the selection among the target hosts" because it is unclear what the distinction is between the selected hosts and "selected ones of the plurality of target hosts which are associated with end-to-end secure network communications[1].

The applicants respectfully traverse these rejections. According to the M.P.E.P. §2173.02, a claim element is definite within the meaning of 35 U.S.C. §112, second paragraph, if the claim language provides at least a *reasonable degree* of particularity and distinctness when considered *as a whole*[2].

For example, Claim 1, *as a whole*, recites that in a distributed workload environment, target hosts are accessed through a common network address by a distribution processor. *Network communications* that are directed to the common network address are *received* at the distribution processor, and the distribution processor distributes the received (inbound) network communications that are directed to the common network address among *selected ones of the target hosts* so as to distribute the workload associated with the network communications among the target hosts.

However, as an example, certain technologies, such as IPSEC, implement network communications as end-to-end secure network communications[3]. Thus, it is possible that some, but not all communications are network secure communications. Accordingly, claim 1 further recites processing both inbound and outbound end-to-end secure network communications at the distribution processor so as to provide endpoint network security processing of communications from the target host and endpoint network security processing of communications to the target host and encapsulating communications between the distribution processor and *selected ones of the plurality of target hosts which are associated with end-to-end secure network communications*.

---

[1] See Office action mailed 10-27-2006, Pages 2-3

[2] See for example, *Orthokinetics, Inc. v. Safety Travel Chairs, Inc.*, 806 F.2d 1565, 1576, 1 USPQ2d 1081, 1088 (Fed. Cir. 1986).

See the applicant's published patent application U.S. Pat. Pub. No. US2002/0095603, paragraph 0022-32. See also, U.S. Pat. No. 6,266,335 to *Bhaskaran*, Col. 2, lines 43-58

In view of the clarifying remarks herein, the applicants believe that, when reading the claim 1 *as a whole*, the claim recitations are definite within the meaning of 35 U.S.C. § 112, second paragraph. The clarifying comments set out in detail above, apply by analogy to independent claims 20, 39. As such, the applicants respectfully request the rejection to claims 1, 20, 39 and the claims that depend therefrom, including claims 3-9, 22-28, 41-47 and 58-72 be withdrawn.

The Art of record Fails to Establish a *Prima Facie* Case of Anticipation

The applicants respectfully assert that *Bhaskaran* fails to teach or suggest one or more elements needed to establish a *prima facie* case of anticipation with regard to each of the rejected claims[4]. For example, Claim 1 recites in pertinent part:

> … processing both inbound and outbound end-to-end secure network communications *at* the distribution processor so as to provide endpoint network security processing of communications from the target host and endpoint network security processing of communications to the target host…

In making the above rejection, the Examiner asserts that the claimed recitation of a distribution processor reads on the flow switch 205 of *Bhaskaran*. The flow switch 205 cannot reasonably be construed as a distribution processor *as claimed*. Moreover, the flow switch 205 actually teaches away from the claimed invention by intentionally not performing endpoint network security processing at the flow switch.

Bhaskaran, discloses a flow switch that can pass IPSEC and other network secure communications that can also perform load balancing of secure packets *by deliberately avoiding* providing "endpoint network security processing of communications" at the flow switch. Traditional load balancers cannot perform load balancing without violating certain network secure processing protocols, e.g., IPSEC or other encrypted packet technologies, because such load balancers do not have access to the non-public crypto-key required to decrypt the IP (layer 3) payload that carries the transport layer information often used for load balancing[5]. *Bhaskaran*, avoids this problem by routing packets using only layer 2 information that does not affect network secure encryption.

[4] See for Example, the M.P.E.P. §706.02(j).
[5] See for example, *Bhaskaran*, Col. 2, line 43-65.

The format of a packet 300 transmitted over an external network is illustrated in FIG. 3A of *Bhaskaran*[6]. To perform load balancing, the flow switch 205 selects a server from the cluster to receive a communication from a client and routes packets to the selected server by writing the MAC address (Layer 2) of the selected server into the Data Link Layer destination address[7] (field 390 of each packet 300 as seen in Fig. 3B corresponding to the link field 320 in Fig. 3A)[8]. Referring to Fig. 3A and as noted in *Bhaskaran*:

> ... If IP header 330 were modified... the checksum for CRC field 360 would have to be recalculated, an operation requiring processor intervention. In addition, if encrypted information is transmitted according to the IPSEC security framework, decryption of the IP payload is required. *Thus, by eliminating the need to recompute the checksum for each packet*, the network flow switch of the present invention achieves better throughput than prior art devices. Network owners can further deploy IPSEC security mechanisms transparently and without fear of communications being broken[9]. (emphasis added)

In other words, as seen in Fig. 1 of *Bhaskaran*, each server has a unique IP address. In order to route packets to one of the servers in Fig. 1, the IP address field 330 (see Fig. 3A) would need to be changed. This would require that the CRC (checksum field 360 in Fig. 3A) be recomputed. However, to re-compute the checksum, the payload (field 350 in Fig. 3A) would need to be decrypted and read to compute the new CRC value. However, a decryption key is unavailable[10] to decrypt the payload.

However, in *Bhaskaran*, each of the servers 210-250 in a cluster 200 share *the same virtual IP address*, e.g., see (layer 3) IP address 290 (192.31.65.1 in the example of Fig. 2) for each server 210-250, but have a distinct Data Link Layer address[11] that is known to the flow switch 205, i.e., a different (layer 2) MAC address (126.1-126.5 in the example of Fig. 2). This is different from the disclosed prior art arrangement where a "load balancer" 100 is coupled to a server cluster where each server has a unique IP (layer 3) address (192.31.65.1 - 192.31.65.5) as seen in Fig. 1.

The layer 2 MAC address *is not* part of the encrypted portion (payload field 360 in Fig. 3A) of a network secure packet and *is not* utilized in the computation of the checksum of the packet (CRC field 360 in Fig. 3A). Thus, IPSEC and other encryption based technologies are unaffected by the decisions of the flow

[6] See for example, *Bhaskaran*, Col. 6, lines 27-50.
[7] See for example, *Bhaskaran*, Col. 5, lines 34-37.
[8] See for example, *Bhaskaran*, Col. 5, lines 56-63.
[9] See for example, *Bhaskaran*, Col. 6, lines 38-50.
[10] See for example, *Bhaskaran*, Col. 2, lines 58-65.

switch. The "better throughput" noted by *Bhaskaran* is derived from the observation that the flow switch 205 can simply *pass* packets with encrypted payloads to the assigned IP server *without providing* endpoint network security processing as claimed because it never modifies the IP address, payload or checksum or performs other time intensive tasks.

Bhaskaran further notes that network owners can further "deploy IPSEC security mechanisms transparently and without fear of communications being broken". Because the flow switch 205 does not have to peek into the packet payload or otherwise have to modify the IP address to perform load balancing, broken communications and other interoperability issues with network secure communications are transparent because the flow switch merely passes packets to the endpoint server in the cluster so that the *server is* the endpoint for secure communication. Since the link field 320 containing the (layer 2) MAC address is not part of the fields computed in the checksum for CRC field 360 when link field 320 is modified[12], there is no "fear of communications being broken".

Bhaskaran fails to teach or suggest processing both inbound and outbound end-to-end secure network communications at the distribution processor so as to provide endpoint network security processing of communications from the target host and endpoint network security processing of communications to the target host, as claimed. Accordingly, the applicants respectfully request this rejection be withdrawn. Claims 20 and 39 recite similar limitations, and thus the above arguments apply by analogy. The remainder of the claims rejected under §102(e) and §103(a) are patentable, at least by virtue of depending from base claims, which the applicants have established are patentable over the cited art.

Conclusion

No *prima facie* case of anticipation or obviousness has been established, and the rejection based upon §112, second paragraph has been adequately clarified. As such, the applicants respectfully request allowance of the pending claims.

Respectfully submitted,
Stevens & Showalter, L.L.P.
By /Thomas E. Lees/
Reg. No. 46,867

[11] See for example, *Bhaskaran*, Col. 5, lines 47-54.
[12] See also, *Bhaskaran*, Col. 2, lines 43-65.